CONFIDENTIAL

STAT

24 December 1987

MEMORANDUM FOR: Director of Information Technology, DA

FROM: [redacted] 25X1
Chief, Information Management Staff, DO

SUBJECT: PBX Installation in the DO

REFERENCE: Memorandum from Chief, Information Systems Security Division, OS to Chief, New Building Project Office, OIT; Subject: Meeting on New Building Project Office - PABX Security, dated 16 June 1986

1. There has been considerable concern in the DO about the impact of the PBX on the compartmentation of the Special Computer Center (SCC). As you know, special efforts have been made in the past to ensure that only those users assigned to the DO (with a few exceptions) received access to the SCC.

2. When the twisted wire grid was in use, these persons, and no one else, had terminals connected to the SCC. Since the PBX employs computer controlled electronic switches to make these connections, the DO requested that all SCC users be collocated on one switch. This would obviously reduce the opportunities for "hackers" to gain access to the SCC, since they would first have to arrange for their terminal to be connected to the PBX via that particular switch (or use someone else's terminal). Also, it would reduce the potential damage attendant to data spillage. This one switch was to be electronically isolated from the other switches such that no data could be transferred among them. Thus, any spillage from the SCC would be limited to the subscribers of that one switch.

[redacted] 25X1

CONFIDENTIAL

SUBJECT: PBX Installation in the DO

3. The request for all SCC users to be collocated on one switch was concurred in by OIT's Chief of the New Building Project Office, on 26 June 1986. A portion of the memo documenting this agreement (see reference) is quoted as follows, "It should be pointed out that all DO subscribers will be in one switch, and that there will be no data transferred from the DO switch, only voice transfers." The memo further points out that due to cost constraints, the DO will share that switch with other subscribers (a condition the DO does not object to).

4. It has now come to our attention that the policy of collocating all SCC users on one switch has not been adhered to. We understand that the "DO switch" has been nearly filled to capacity (approximately 4,400 users) by the connection of large numbers of non-SCC users, and the installers now plan to connect SCC users via other PBX switches. We strongly object to this on security grounds and request that all SCC users be placed on one switch as previously agreed.

5. Our requirement is that access to the SCC be firmly restricted to DO authorized users.

25X1

Attachment:
Reference

OIT/TRIS
LOGGED

16 JUN 1986

MEMORANDUM FOR: Chief, New Building Project Office, OIT

FROM: [redacted] 25X1
Information Systems Security Division

SUBJECT: Meeting on New Building Project Office - PABX Security [redacted] 25X1

1. This memorandum will confirm the topics that we discussed, on 29 April 1986, regarding the current status of security of the PABX switches. Attending from the New Building Project Office (NBPO) were [redacted] 25X1
[redacted] and two other members; attending from the Office of 25X1
Security (OS) were [redacted] and 25X1
the undersigned. The purpose of the meeting was to discuss security concerns that have been surfaced in previous correspondence and meetings with NBPO, discuss the status of these concerns, and to discuss and agree on a planned course of action for the security of the digital switches. [redacted] 25X1

2. The two documents that were the basis for the discussion were the Informal Comments from ISSG, dated 27 August 1984, to the RFP, and Appendix C "SC-200 and SC201." [redacted] 25X1

3. The first concern that was discussed centered on "trunk transfers" of the secure switch. Of particular concern in this area has to do with the intentional rerouting of calls which actually appears to be an NSA concern regarding SI clearances. Within the Agency, all individuals utilizing secure phones will have a minimum TS Agency clearance and a SCI SI access approval. It was agreed that the Agency would prohibit the transfer of calls, that originate from outside trunks, to another outside trunk. The Agency will also prohibit the use of call forwarding on the secure switches. [redacted] 25X1

4. It was agreed that ISSD had never requested that audit trail information from the PABX switches and that SMNS data be reformatted and transfered to the Agency mainframe systems. In the area of auditing, we did agree, however, that there is a need to audit the 3270 terminals which calls for port-to-port auditing as opposed to buffer-to-buffer. ISSD has outstanding action item to identify the data elements necessary to perform this type of audit function and deliver these items to the NBPO. [redacted] 25X1

[redacted] 25X1

CONFIDENTIAL

5. Another issue that was raised concerned assurances, specifically Sections 2.5.2(D) and 2.5.2(C) of SC-201. [redacted] 25X1 advised that the plan calls for a deliverable item from Contel outlining what testing procedures will be conducted to insure security of the switch and this plan will be made available for security review. She also suggested that Security could participate in this testing which is an excellent suggestion and one that Security will follow. It was anticipated that the test would basically insure that positive checks in the system do in fact function (e.g., using a fake password to determine how this system responds). [redacted] commented that TRW is hiring a 25X1 Northern Telcom digital specialist to review source code for a digital switch that TRW is installing in one of its classified environments. It should be pointed out, however, that the Agency does not plan to examine source code as part of its test procedures. [redacted] 25X1

6. Another area of discussion focused on the nonsecure switch and the use of modem pools. Steve Sondag advised that, because of the way in which most Agency customers use unclassified circuits (permanent day-long use), it would not be advantageous to use the modem pool. However, the modem pools would provide greater control and accountability and may be considered in the future. [redacted] 25X1

7. The subject of SMNS security was discussed and the fact that the system administrator for the SMNS system should be an Agency staff employee. The group unanimously agreed that this function must be the responsibility of an Agency staffer and should not be delegated to cleared contractor personnel. ISSD will prepare a memo requesting the Office of Information Technology identify an Agency individual to fulfill this function. [redacted] 25X1

8. Another area that was discussed centered around the "host port drop" concern. This concern discusses the security vulnerability that occurs when a switch or Comten loses a connection; the problem being that, when the switch or Comten reconnects, the reconnection be made with the connection and not dynamically allocated to a new connection. This will require modification of the Comten boards which has already been contracted for by the NBPO. [redacted] 25X1

9. [redacted] 25X1 then brought up the conversation that she had with [redacted] 25X1, DO/Information Management Staff, which centered on DO concerns about the switch. Some of the DO concerns centered on the issue of redundancy, and the fact that they want all of the DO on one switch. The entire DO will be on one switch, however, they will share that switch with other subscribers. The only other alternative to this would be to procure a dedicated switch at the cost of approximately $12 million for the DO. It should be pointed out that all DO subscribers will

be in one switch and that there will be no data transfered from the DO switch only voice transfers. The DO is also concerned about the O&M being performed by Contel, and they (DO) want to have data access control (in other words DO wants to control passwords to the SMNS data base). The DO is also concerned about physical access to the center, which we agree should be controlled by staff Agency personnel. The transition from the Comten to the IBX is also a DO concern in terms of the Agency's ability to continue to audit, e.g., terminal to host connections.

25X1

10. The undersigned asked if there are any security requirements that are in Appendix C that we (OIT or OS) cannot do? The only area that we agreed upon that we would not be able to complete is the review of source code for the IBX. With over 500,000 lines of source code to review, it appears fairly unrealistic to perform this type of analysis on the source code, human resources not withstanding, and then perform a similar analysis on PTF (program temporary fix). Other than the source code analysis, all other security requirements will be met.

25X1

11. Based on the security concerns, and corresponding responses from NBPO and ISSD, outlined in this memorandum, I believe that OS and OIT are in agreement with respect to the security features, physical, procedural and technical, that can be implemented based on the state-of-the-art in the timeframe for bringing on-line an off-the-shelf PABX system. We agreed that as technology progresses and additional security features become available in upgrades to existing systems, e.g., B-1 level VAX system proposed by DEC to be available by FY 1987, such new technologies will be incorporated in Agency scheduled upgrades where possible. Also, ISSD will survey the existing market to determine if there are add on security packages available, e.g., the ACF2-like technology, for PABX switches. If such a package is located, consideration will be given to implementing on Agency systems subject to available funds and appropriate functional analysis and testing.

25X1

25X1

CONCUR:

25X1

Chief, New Building Project Office
Office of Information Technology

6/26/86
Date

O/D/OIT Routing Slip

Date 1-4-88

	Action	Info	Seen
D		✓	
DD			
Nancy			
Rose			
Mary			
C/CSG			
C/DG			
C/EG	✓		
C/MG			
C/OG			
D/CSPO			
SADE			
C/A&TPS			
C/TSS			

COMMENT:

action: C/EG 11 Jan

info cy - C/CSG